Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Mario M. Choi (SBN 243409)
KAPLAN FOX & KILSHEIMER LLP
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
lking@kaplanfox.com
mchoi@kaplanfox.com

Joel B. Strauss (*pro hac vice* to be filed)
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue, 14th Floor
New York, NY 10022
Telephone: 212-687-1980
Facsimile: 212-687-7714
jstrauss@kaplanfox.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

J. Doe, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

HEALTH NET OF CALIFORNIA, INC., HEALTH NET, LLC, and ACCELLION, INC., a Delaware Corporation,

Defendants.

Case No. 21-cv-2975

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff J. Doe ("Plaintiff"), by and through their attorneys[1], individually and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendants Health Net of California, Inc., Health Net, LLC (collectively "Health Net") and Accellion, Inc., a Delaware corporation ("Accellion" and with Health Net, "Defendants"), and makes the following allegations based upon knowledge as to themselves and their own acts, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Accellion is a software company that provides third-party file transfer software and services to clients. Accellion touts itself as enabling "millions of executives, employees, customers, vendors, partners, investors, attorneys, doctors, patients, and professionals from every walk of life to do their jobs without putting their organizations at risk. When they click the Accellion button, they know it's the safe and secure way to share information with the outside world."[2]

2. Health Net is a nationwide healthcare conglomerate that provides insurance through HMO and PPO plans to patients, including many that are enrolled through government funded programs such as Medicare, Medicaid, and Veterans Affairs Programs.

3. Accellion makes and sells a file transfer service called File Transfer Appliance ("FTA"), a product specializing in large file transfers. Accellion's FTA software is a 20-year-old

[1] Plaintiff Doe is proceeding pseudonymously so that their medical information and HIV status is not further compromised and to reduce the risk of housing, healthcare and employment discrimination traditionally experienced by those with or at high risk of contracting HIV and/or AIDS. This is permissible under Ninth Circuit law. *Does I thru XXIII v. Advanced Textile Corp.*, 214 F. 3d 1058 (9th Cir. 2000); *see also Doe v. Kaweah Delta Hospital*, No. 1:08-cv-0118-AWI-GSA (E.D. Cal. Aug. 15, 2016); *Doe v. Megless*, 654 F.3d 404, 408-9 (3d Cir. 2011) (endorsing a noncomprehensive balancing test, which balances, "whether a litigant has a reasonable fear of severe harm that outweighs the public's interest in open litigation," and including AIDS as an example of an area where courts have permitted plaintiffs to proceed with pseudonyms); *Smith v. Milton Hershey Sch.*, No. CIV.A. 11-7391 (E.D. Pa. 2011) (allowing mother of HIV-positive minor child to proceed under pseudonym); *Doe v. Deer Mountain Day Camp, Inc.*, No. 07-cv- 5495 (S.D.N.Y. Jun. 22, 2007) (permitting minor and his parent alleging HIV discrimination against camp to proceed under pseudonym); *EW v. New York Blood Center*, 213 F.R.D. 108, 110 (E.D.N.Y. 2003) (holding that the prejudice of embarrassment and fear of stigmatization because plaintiff had a "sexually and blood-transmitted disease" like AIDS "is real."). Plaintiff Doe is using they/them pronouns to avoid disclosure of their gender identity.

[2] *See Secure Risky Third Party Communications While Saving Money*, Accellion, https://www.accellion.com/platform/simple/secure-third-party-communication/ (last visited April 23, 2021).

legacy product that was "nearing end-of life."[3] Indeed, Accellion had announced that, while it would continue supporting and honoring its FTA contracts for the duration of its existing License Terms, the obsolete FTA software End of Life would be effective April 30, 2021.[4] Accellion had "encouraged all FTA customers to migrate to Kiteworks [Accellion's current file transfer software] for the last three years." *Id.*

4. Because Accellion's FTA software was obsolete and otherwise nearing its end of life, it was vulnerable to compromise and security incidents. And, that security incident came to fruition in mid-December 2020, when Accellion was made aware of the FTA's vulnerabilities as unauthorized third parties compromised the FTA software and gained access to Accellion's clients' files (the "Data Breach").

5. It was not until January 12, 2021 that Accellion announced that an unauthorized individual gained access to certain files and data of numerous customers of Accellion had stored on and shared through Accellion's FTA software.[5] This unauthorized access began in December 2020 and continued into January 2021.

6. Companies that were affected by the Data Breach include the Washington State Auditor's Office, the University of Colorado, Jones Day, Goodwin Procter, Kroger, and Defendant Health Net.

7. On January 25, 2021, Health Net was notified by Accellion of the Data Breach and that certain Health Net files were accessed. However, Health Net only began advising customers of its Data Breach on or about March 24, 2021—*two months later*.

8. The compromised Health Net files and data included names, home addresses, insurance ID numbers, and "health information, such as your medical condition(s) and treatment

---

[3] *See Accellion Provides Update to Recent FTA Security Incident*, Accellion (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

[4] *See Graduate from Secure File Transfer to Secure 3rd Party Content Communication: Accellion FTA*, Accellion, https://www.accellion.com/products/fta/ (last visited April 23, 2021).

[5] *See Accellion Responds to Recent FTA Security Incident*, Accellion, (Jan. 12, 2021), https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/.

information."[6] Other Accellion business partners like Kroger's pharmacies also had significant information disclosed, such as Social Security numbers, information used to process insurance claims, and health information such as prescription information and medical history (collectively "Personally Identifiable Information" or "PII" and/or "Personally Identifiable Health Information" or "PHI").[7]

9. Defendants were well aware of the data security shortcomings in the FTA product. Nevertheless, Accellion continued to use FTA with its clients, putting Accellion's file transfer service clients and their clients' customers and employees at risk of being impacted by a breach.

10. Defendants' failure to ensure that its file transfer services and products were adequately secure fell far short of its obligations and Plaintiff's and Class Members' reasonable expectations for data privacy, had jeopardized the security of their PII/PHI, and has put them at serious risk of fraud and identity theft. Indeed, Plaintiff Doe has already been informed that their information has been made available for sale on the dark web.

11. Defendants also failed to ensure that Plaintiff's and Class Members' reasonable expectations for data privacy would be maintained, jeopardizing the security of their PII/PHI and putting them at serious risk of fraud and identity theft, by failing to adequately maintain the security of Plaintiff's and Class Members' PII/PHI or upgrading software given Accellion's notice and Health Net's knowledge that the FTA software's end-of-life would be effective April 30, 2021.

12. Plaintiff brings this class action alleging that Defendants' conduct, as described more fully herein, caused Plaintiffs' and others' PII/PHI to be exposed and stolen because of the failure of Defendants to safeguard and protect their sensitive information. Plaintiff seeks damages, and injunctive and other relief, on behalf of theirself and similarly situated consumers.

---

[6] *See* https://www.healthnet.com/content/healthnet/en_us/news-center/news-releases/cyber-accellion.html

[7] *See* Chris Mayhew, *Kroger advises customers of a data breach affecting pharmacy and Little Clinic*, Cincinnati Enquirer, (Feb. 19, 2021 8:34 p.m.), https://www.cincinnati.com/story/news/2021/02/19/kroger-warns-customers-medical-prescriptions-data-breach/4514664001/. *See also Accellion Security Incident Impacts Kroger Family of Companies Associates and Limited Number of Customers*, (Dec. 19, 2021), http://ir.kroger.com/CorporateProfile/press-releases/press-release/2021/Accellion-Security-Incident-Impacts-Kroger-Family-of-Companies-Associates-and-Limited-Number-of-Customers/default.aspx.

PARTIES

13. Plaintiff J. Doe is a resident of San Francisco, California. They received a notice letter from Health Net dated March 24, 2021 stating that their PHI/PII, including their medical condition and treatment, was compromised by the Data Breach.

14. Defendant Health Net of California, Inc., is a California corporation with its principal place of business in Woodland Hills, California.

15. Defendant Health Net, LLC, is a Delaware Corporation that is the parent corporation of Health Net of California, Inc., and maintains its headquarters in Woodland Hills, California, and St. Louis, Missouri.

16. Defendant Accellion, Inc., is a Delaware corporation headquartered in Palo Alto, California.

JURISDICTION AND VENUE

17. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

18. This Court has personal jurisdiction over Accellion and Health Net of California because they are headquartered in California, are authorized to do business and do conduct business in California, have specifically marketed, advertised, and made substantial sales in California, and have sufficient minimum contacts with this state and/or sufficiently avail themselves of the markets of this state through its promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible.

19. This Court has personal jurisdiction over Health Net, LLC because it does conduct business in California through its subsidiaries such as Health Net of California, has specifically marketed, advertised, and made substantial sales in California, and has sufficient minimum contacts with this state and/or sufficiently avails itself of the markets of this state through its promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible.

20. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendants do substantial business in this District, have intentionally availed themselves of the laws and markets within this District through their promotion, marketing, distribution and sales activities in this District, and a significant portion of the facts and circumstances giving rise to Plaintiff's Complaint occurred in or emanated from this District.

21. Pursuant to Civil Local Rule 3-2(c), an intra-district assignment to the San Jose Division is appropriate because a substantial part of the events or omissions which give rise to the claims asserted herein occurred in this Division, including that Accellion is headquartered and located in Santa Clara County.

FACTUAL ALLEGATIONS

A. Background

22. Health Net is a nationwide healthcare conglomerate that provides insurance through HMO and PPO plans to patients, including many that are enrolled through government funded programs such as Medicare, Medicaid, and Veterans Affairs Administration.

23. Health Net has had a prior history of incidents with the loss and exposure of digital electronic records. In 2009, Health Net's Connecticut affiliate lost a portable hard drive with a terabyte of data that contained PII/PHI of 1.5 million policy holders. Due to that incident, Health Net was sued by the states of Vermont and Connecticut for violating the states' security breach notification laws and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d, *et seq.* Due to the scope of the loss of data, and the deliberate delay of disclosure, Health Net agreed to pay damages and fines and offered stronger consumer protections moving forward.

24. Two years later, in January 2011, Health Net was informed by its IT vendor, IBM, that nine servers at a Rancho Cordova, California facility went missing, containing PHI and medical records for 1.9 million customers. Health Net did not notify customers for over two months, beginning on March 14, 2011. Health Net was subject to investigations by the California Department of Managed Care, the California Department of Insurance, the Connecticut Attorney General, and the Oregon Department of Consumer and Business Services' Division of Finance and Corporate

Securities. Health Net was also sued in a series of class action lawsuits brought by impacted patients in state and federal court, which resulted in a multi-million dollar settlement for compensation and credit monitoring services to class members, and operational changes intended to prevent future data loss incidents. In December 2014, Health Net also entered into a Settlement Agreement with the State of California Department of Managed Care to pay a $200,000 fine and take additional measures to ensure the privacy and security of its patients' medical records.[8]

25. Accellion is a company that makes, markets, and sells file transfer platform software and services.

26. Accellion touts that its software "prevents data breaches and compliance violations from third party cyber risk."[9] Specifically, Accellion touts that its FTA software purportedly "helps worldwide enterprises … transfer large and sensitive files securely using a 100% private cloud, on-premise, or hosted."[10]

27. Accellion's FTA software was used by Health Net to store, secure, and transfer Plaintiff's and Class Members' most sensitive and confidential information, including names, Social Security numbers and/or health insurance numbers, dates of birth, privileged and confidential documents, health records, medical treatment information, and other personal identifiable information.

28. Plaintiff and Class Members relied on Defendants to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII/PHI from involuntary disclosures to third parties.

29. Accellion acknowledged that its FTA software was a "legacy" product,[11] outdated and was "nearing end-of-life,"[12] thereby leaving it vulnerable to compromise and security incidents.

---

[8] *See* https://wpso.dmhc.ca.gov/enfactions/docs/2214/1602277464557.pdf

[9] *See About Accellion*, Accellion, https://www.accellion.com/company/ (last visited April 23, 2021).

[10] *See Graduate from Secure File: Transfer to Secure 3rd Party Content Communication*.

[11] *Accellion Responds to Recent FTA Security Incident*.

[12] *Accellion Provides Update to Recent FTA Security Incident*.

30. Nonetheless, Health Net continued using Accellion's FTA software, despite receiving notice that Accellion's FTA software was outdated and was "nearing end-of-life," and further receiving notification that it should upgrade to other software, including Accellion's "Kiteworks®" platform.

B. The Data Breach

31. On January 12, 2021, Accellion issued a statement concerning the Data Breach, indicating that, in mid-December 2020, it "was made aware of a P0 vulnerability in its legacy File Transfer Appliance (FTA) software."

32. A "P0 vulnerability" or "zero-day vulnerability" is a newly discovered software security flaw that is known to the software vendor but does not have a patch in place to fix the flaw.[13] "Zero-day" refers to the fact that a developer has "zero-days" to fix the problem that was exposed and may have already been exploited by hackers. *Id.*

33. Accellion indicated in its January 12, 2021 press release that it had "resolved the vulnerability and released a patch within 72 hours to the less than 50 customers affected."[14]

34. On February 1, 2021, Accellion issued a press release providing an update concerning the Data Breach.[15] Accellion represented that it "patched all known FTA vulnerabilities exploited by the attackers and has added new monitoring and alerting capabilities to flag anomalies associated with these attack vectors." *Id.*

35. While Accellion was made aware of the Data Breach in mid-December, Accellion acknowledged that the "initial incident was the beginning of a concerted cyberattack on the Accellion FTA product that continued into January 2021." *Id.* Accellion "rapidly developed and released patches to close each vulnerability," and continued to "work closely with FTA customers to mitigate the impact of the attack and to monitor for anomalies." *Id.*

---

[13] *See* Kyle Chivers, *Zero-day vulnerability: What it is, and how it works*, Norton, (Aug. 28, 2019), https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.

[14] *Accellion Responds to Recent FTA Security Incident*.

[15] *Accellion Provides Update to Recent FTA Security Incident*.

36. As Frank Balonis, Accellion's Chief Information Security Officer, conceded, "[f]uture exploits, however, are a constant threat." *Id.* And Accellion has attempted to deflect responsibility for the incident, stating that it has encouraged customers to upgrade their platform for three years. *Id.* Accellion also stated that it contracted with Mandiant, a cybersecurity forensics firm, to conduct a compromise assessment. *Id.*

37. On February 22, 2021, Accellion issued a statement regarding Mandiant's preliminary findings.[16] Mandiant identified UNC2546 as the criminal hacker behind the cyberattacks and data theft involving the FTA software.[17]

38. Multiple Accellion FTA customers received extortion emails from UNC2546, threatening to publish stolen data on the "CL0P^_-LEAKS".onion website. *Id.* Further, some of the published victim data appeared to have been stolen using the DEWMODE web shell. *Id.* Mandiant is continuing to track the subsequent extortion activity. *Id.*

C. Notification of Accellion's FTA Customers

39. In its February 1, 2021 press release, Accellion indicated that "[a]ll FTA customers were promptly notified of the attack on December 23, 2020."[18]

40. However, on or around January 25, 2021, the Australian Securities and Investments Commission announced that it was one of the customers affected by the Data Breach,[19] having become aware of the Data Breach on January 15, 2021 when its server was accessed on December 28, 2020. This raises doubt as to whether Accellion notified all of its customers of the Data Breach on December 23, 2020, as Accellion claimed it did.

---

[16] *See Accellion Provides Update to FTA Security Incident Following Mandiant's Preliminary Findings*, Accellion, (Feb. 22, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-fta-security-incident-following-mandiants-preliminary-findings/.

[17] *See* Moore, et al., *Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion*, FireEye, (Feb. 22, 2021), https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html.

[18] *See Accellion Provides Update to Recent FTA Security Incident.*

[19] *See Accellion cyber incident*, Australian Securities & Investments Commission, https://asic.gov.au/about-asic/news-centre/news-items/accellion-cyber-incident/ (last visited April 23, 2021)

41. On or around February 1, 2021, the Office of the Washington State Auditor announced that it was one of the customers affected by the Data Breach, having received confirmation by Accellion "[d]uring the week of January 25, 2021 … that an unauthorized person gained access to S[tate] A[uditor] O[ffice] files by exploiting a vulnerability in Accellion's file transfer service."[20] This raises doubt as to whether Accellion notified all of its customers of the Data Breach on December 23, 2020, as Accellion claimed it did.

42. On or around February 9, 2021, the University of Colorado announced that it was affected by the Data Breach.[21] The University of Colorado indicated that it suspended use of the FTA software on January 25, 2021, raising doubt as to whether Accellion notified all of its customers of the Data Breach on December 23, 2020, as Accellion claimed it did.

43. On or around February 11, 2021, Singtel was informed by Accellion that the FTA software "has been illegally attacked by unidentified hackers."[22] This raises doubt as to whether Accellion notified all of its customers of the Data Breach on December 23, 2020, as Accellion claimed it did.

44. Other companies domestically and internationally, including QIMR Berghofer Medical Research Institute,[23] the Reserve Bank of New Zealand,[24] Jones Day,[25] and Goodwin Proctor,[26] were all affected by the Data Breach.

---

[20] *See About the Accellion data security breach*, Office of the Washington State Auditor, https://sao.wa.gov/breach2021/(last visited April 23, 2021)

[21] *See About the Accellion Cyberattack*, University of Colorado, (Feb. 12, 2021), https://www.cu.edu/accellion-cyberattack.

[22] *See About Accellion FTA Security Incident*, Singtel, https://www.singtel.com/personal/support/about-accellion-security-incident (last visited April 23, 2021)

[23] *See QIMR Berghofer investigates suspected Accellion data breach*, QIMR Berghofer Medical Research Institute, https://www.qimrberghofer.edu.au/media-releases/qimr-berghofer-investigates-suspected-accellion-data-breach/ (last visited April 23, 2021).

[24] *See Our response to Data Breach*, Reserve Bank of New Zealand, https://www.rbnz.govt.nz/our-response-to-data-breach (last visited April 23, 2021).

[25] Chris Opfer, *Jones Day Hit by Data Breach as Vendor Accellion Hack Widens*, Bloomberg Law, (Feb. 16, 2021, 4:30 p.m.), https://news.bloomberglaw.com/business-and-practice/jones-day-hit-by-data-breach-as-vendor-accellion-hacks-widen.

[26] Meghan Tribe, *Goodwin Procter Says It Was Hit by Data Breach of Vendor (1)*, Bloomberg Law, (Feb. 2, 2021, 12:36 p.m.), https://news.bloomberglaw.com/business-and-practice/goodwin-procter-says-it-was-hit-by-data-breach-of-vendor.

D. Health Net Announces It was Impacted by the Data Breach

45. On January 25, 2021, Health Net was informed that the PII/PHI of its patients was part of the Accellion breach. On March 24, 2021, Health Net publicly acknowledged the incident and confirmed that the breach happened between January 7 and January 25, 2021, and that patients' names, addresses, dates of birth, insurance ID numbers, and health information, including medical condition(s) and treatment information were compromised. Health Net began informing patients via letter, offering one year of credit monitoring through IDX and encouraging patients to take additional steps to review their credit and account information.

E. Impact of the Data Breach

46. The Data Breach creates a heightened security concern for Health Net patients such as Plaintiff and Class Members because their PII/PHI, including unique medical records and other sensitive health and prescription information was included.

47. Medical privacy is among the most important tenets of American healthcare. Patients must be able to trust their physicians, insurers, and pharmacies to protect their medical information from improper disclosure including, but not limited to, their health conditions and courses of treatment. Indeed, numerous state and federal laws require this. And, these laws are especially important when protecting individuals with particular medical conditions such as HIV or AIDS that can and do subject them to regular discrimination.

48. Defendants' conduct is especially egregious in this instance because it impacted individuals historically subject to discrimination based upon their medical condition. Although many would like to believe a lot has changed since the U.S. Supreme Court held in 1998 that HIV/AIDS was subject to protections of the Americans with Disabilities Act[27], persons living with HIV and those at high risk of infection continue to battle for equal access to healthcare and rights.

49. In a 2009 survey by Lambda Legal, "nearly 63 percent of the respondents who had HIV reported experiencing one or more of the following types of discrimination in health care: being refused needed care; being blamed for their healthcare status; and/or a healthcare

[27] *Bragdon v. Abbott*, 524 U.S. 624 (1988).

professional refusing to touch them or using excessive precautions, using harsh or abusive language, or being physically rough and abusive."[28] Of those surveyed, 19% reported being denied care altogether.

50. Persons living with HIV (and their families) are also regularly subjected to employment and housing discrimination. In the 2000s, the U.S. Equal Employment Opportunity Commission received 2,175 complaints of discrimination based on HIV, with complaints peaking in the last year of the survey, demonstrating a disturbing upward trend. And, a 2009 national survey conducted by the Kaiser Foundation also showed that only 21% of people were comfortable living with someone with HIV. There are also numerous reported lawsuits over instances in which individuals with HIV (including children) have been denied housing and equal access because of their HIV status.

51. It is also well known that HIV and AIDS disproportionately impacts minority groups such as the LGBT community and African Americans. According to AmFAR, gay and bisexual men accounted for 82% of the United States' 1.2 million people living with HIV, with African-Americans accounting for 45% of HIV diagnoses but only 12% of the general population.[29]

52. The pervasive discrimination suffered by those with HIV or AIDS leads to a social stigma that results in significant harm, including a direct correlation to higher rates of depression, loneliness, and social isolation—and results in those suffering from (or at high risk of) the illness to avoid testing and treatment to avoid the negative consequences of a positive diagnoses.

53. In addition to harms associated with the disclosure of a person's HIV status, the Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things,

[28] https://www.lambdalegal.org/sites/default/files/publications/downloads/fs_hiv-stigma-and-discrimination-in-the-us_1.pdf, last accessed May 8, 2018. All statistics cited herein are taken from Lambda's report unless otherwise attributed.

[29] http://amfar.org/About-HIV-and-AIDS/Facts-and-Stats/Statistics--United-States/, last accessed April 23, 2021.

"[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

54. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. Indeed, the Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[30]

55. It is also difficult to obtain a new Social Security number. A breach victim would have to demonstrate ongoing harm from misuse of her Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

56. Given the highly sensitive nature of Social Security numbers, theft of these numbers in combination with other personally identifying information may cause damage to victims for years.

57. Defendants had a duty to keep PII/PHI confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their PII/WHI to Health Net with the understanding that Health Net and any business partners to whom Health Net disclosed PII would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

58. Defendants' data security obligations were particularly important given the substantial increases in data breaches in recent years, which are widely known to the public and to anyone in Accellion's industry of data collection and transfer.

59. Data breaches are not new. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that

[30] *Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 23, 2021).

data privacy and security is adequate to protect against and prevent known attacks. Indeed, Health Net has been subject to numerous data security incidents, as have other healthcare conglomerates such as Anthem and Premera Blue Cross.

60. It is well known among companies that store sensitive personally identifying information that sensitive information is valuable and frequently targeted by criminals.

61. Identify theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

62. There may be a time lag between when the harm occurs versus when it is discovered, and also between when PII/WHI is stolen and when it is used. According, to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

63. With access to an individual's PII/PHI, criminals can commit all manners of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information.

64. PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen Social Security numbers and other PII/WHI directly on various illegal websites making the information publicly available, often for a price.

[31] *Report to Congressional Requesters*, U.S. Government Accountability Office, (June 2007), http://www.gao.gov/new.items/d07737.pdf.

65. Moreover, a study found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[32]

66. Accellion is, and at all relevant times has been, aware that the sensitive PII/PHI it handles and stores in connection with providing its file transfer services is highly sensitive. As a company that provides file transfer services involving highly sensitive and identifying information, Accellion is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

67. Accellion was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with failing to ensure that its file transfer product FTA was adequately secured, or phasing out the platform altogether.

68. Health Net is, and at all relevant times has been, aware that the sensitive PII/PHI it handles and stores is highly sensitive. As a company that handles highly sensitive and identifying medical information, Health Net is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

69. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable data breaches, Defendants failed to take reasonable steps to adequately protect its systems from being breached and to properly phase out its unsecure FTA platform, leaving its clients and all persons who provide sensitive PII/PHI to its clients exposed to risk of fraud and identity theft.

70. The security flaws inherent to Accellion's FTA file transfer platform—and continuing to market and sell a platform with known, unpatched security issues—run afoul of industry best practices and standards. Had Accellion adequately protected and secured FTA, or stopped supporting the product when it learned about its vulnerabilities, it could have prevented the Data Breach.

[32] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010, 5:00 a.m.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims; see Annie Nova, *Here's how to avoid medical identity theft*, CNBC, (June 7, 2019 11:15 a.m.), https://www.cnbc.com/2019/06/07/how-to-avoid-medical-identity-theft.html.

71. Accellion had put its customers on notice in that it was encouraging its customers to upgrade to another of Accellion's platforms. Because Health Net received notice that Accellion was no longer supporting the FTA software and had been advised to upgrade to new or different software, Health Net was aware, or should have been aware, that it was at risk of using "legacy" software that was subject to breach.

72. Despite the fact that Defendants were on notice of the possibility of data theft associated with the FTA platform, it still failed to make necessary changes to the product or to stop offering and supporting it, and permitted a massive intrusion to occur that resulted in the FTA platform's disclosure of Plaintiffs' and Class members' PII/PHI to criminals.

73. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; disclosure of their medical conditions and courses of treatment; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PII/PHI; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of PII/PHI.

74. Victims of the Data Breach have likely already experienced harms, which is made clear by news of attempts to exploit this information for money by the hackers responsible for the breach.[33] Indeed, an UNC-2582 extortion email similar to the following has been received by at least one victim of the Data Breach:

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30

[33] *See Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion.*

> thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.[34]

75. As a result of Accellion's failure to ensure that its FTA product was protected and secured, or to phase out the platform upon learning of FTA's vulnerabilities, the Data Breach occurred. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their PII/PHI is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

76. As a result of Health Net's failure to heed Accellion's warning to upgrade, due in part to Accellion's FTA product being subject to vulnerabilities and Accellion was phasing out the platform, the Data Breach occurred. As a result of the Data Breach, Plaintiff and Class Members' privacy has been invaded, their PII is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PLAINTIFF'S EXPERIENCES

77. Plaintiff J. Doe learned of the Data Breach via a notice by Health Net received on or about April 1, 2021.

78. Plaintiff J. Doe has been enrolled in Health Net's insurance coverage services since approximately 2006, including for treatments associated with their living with HIV for over 20 years.

79. As a result of learning of the Data Breach, Plaintiff Doe spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring their accounts. In fact, on April 3, 2021, Plaintiff Doe was informed by a credit monitoring service that their information was available on the dark web.

[34] *Id.*

80. Plaintiff Doe suffered actual injury in the form of damages to and diminution of the value of his/her PII/PHI – a form of intangible property that Plaintiff Doe entrusted to Defendants for the purpose of obtain medical care, which was compromised in and as a result of the Data Breach.

81. Plaintiff Doe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

82. Plaintiff Doe has suffered imminent and impending injury arising from the disclosure of their HIV status and treatment and for the substantially increased risk of fraud, identity theft, and misuse resulting from their PII/PHI, especially their insurance identification number and medical information, in combination with their other PII/PHI, being placed in the hands of unauthorized third parties and criminals.

83. Plaintiff Doe has a continued interest in ensuring that their PII/PHI, which remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of theirself and all members of the following nationwide class (the "Accellion Class"):

> All persons in the United States whose PII/PHI was exposed to unauthorized third parties as a result of the compromise of Accellion FTA that occurred between December 2020 and January 2021 (the "Accellion Class").

Plaintiff reserves the right to modify, change, or expand the Accellion Class definition, including proposing additional subclasses, based on discovery and further investigation.

85. Plaintiff further brings a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of theirself and all members of the following nationwide class (the "Health Net Class"):

> All persons in the United States who are Health Net subscribers whose PII/PHI was exposed to unauthorized third parties as a result of the compromise of Accellion FTA that occurred between December 2020 and January 2021 (the "Health Net Class").

Plaintiff reserves the right to modify, change, or expand the Health Net Class definition, including proposing additional subclasses, based on discovery and further investigation.

86. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants have a controlling interest, and its current or former employees, officers, and directors; (3) counsel for Plaintiffs and Defendants; and (4) legal representatives, successors, or assigns of any such excluded persons.

87. The Classes meet all of the criteria required by Federal Rule of Civil Procedure 23(a).

88. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it appears that the membership of the Classes are in the tens of thousands. The identities of Class members are also ascertainable through Defendants' records.

89. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether and to what extent Defendants had a duty to protect the PII/PHI of Plaintiff and Class Members;

(b) Whether Defendants failed to adequately safeguard the PII/PHI of Plaintiff and Class Members;

(c) Whether and when Defendants actually learned of the Data Breach;

(d) Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII/PHI had been compromised;

(e) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(f) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(g) Whether Defendants were negligent or negligent per se;

(h) Whether Defendants violated the California Consumer Privacy Act, California Confidentiality in Medical Information Act and California's Unfair Competition Law;

(i) Whether Plaintiff and Class Members are entitled to relief from Defendants as a result of Defendants' misconduct, and if so, in what amounts; and

(j) Whether Class members are entitled to injunctive and/or declaratory relief to address the imminent and ongoing harm faced as a result of the Data Breach.

90. **Typicality:** Plaintiff's claims are typical of the claims of the Classes they seek to represent, in that the named Plaintiff and all members of the proposed Classes have suffered similar injuries as a result of the same misconduct alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Classes.

91. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Classes and has retained attorneys well experienced in class actions and complex litigation as their counsel, including cases alleging breach of privacy and negligence claims arising from corporate misconduct.

92. The Classes also satisfy the criteria for certification under Federal Rule of Civil Procedure 23(b) and 23(c). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendants; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendants have acted or refused to act on grounds that apply generally to the proposed Classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Classes as a whole; that questions of law or fact common to the Classes predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff also avers that certification of one or more subclasses or issues may be appropriate for certification under Federal Rule of Civil Procedure 23(c).

Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Classes will not be difficult.

93. Plaintiff and other members of the Classes have suffered damages as a result of Defendants' unlawful and wrongful conduct. Absent a class action, Defendants' unlawful and improper conduct shall, in large measure, not go remedied. Absent a class action, the members of the Classes will not be able to effectively litigate these claims and will suffer further losses.

CLAIMS FOR RELIEF

COUNT I
Negligence

94. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

95. Accellion negligently sold its FTA product which it has acknowledged is vulnerable to security breaches, despite representing that the product could be used securely for large file transfers. Health Net negligently used FTA for the storage and transmission of PII/PHI

96. Defendants were entrusted with, stored, and otherwise had access to the PII/PHI of Plaintiff and Class Members.

97. Defendants knew, or should have known, of the risks inherent to storing the PII/PHI of Plaintiff and Class Members, and to not ensuring that the FTA product was secure. These risks were reasonably foreseeable to Defendants, because Accellion had previously recognized and acknowledged the data security concerns with its FTA product.

98. Defendants owed duties of care to Plaintiff and Class Members whose PII/PHI had been entrusted to them.

99. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security in connection with marketing, sale, and us of the FTA product. Defendants had a duty to safeguard Plaintiff's and Class Members' PII and to ensure that their systems and products adequately protected PII.

100. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

101. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' PII/PHI.

102. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII/PHI.

103. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

104. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

105. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se

106. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

107. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Defendants had a duty to provide adequate data security practices, including in connection with its sale of its FTA software, to safeguard Plaintiff's and Class Members' PII/PHI.

108. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d, *et seq.*, Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Member's PII/PHI.

109. Pursuant to other state and federal laws requiring the confidentiality of PII/PHI, including, but not limited to, California Confidentiality in Medical Information Act ("CMIA"), Cal. Civ. Code. §§ 56, *et seq.*, and California's HIV Disclosure Laws, Cal. Health & Safety Code § 120980, Defendants had a duty to implement reasonably safeguards to protect Plaintiff's and Class Members' PII/PHI.

110. Defendants breached their duties to Plaintiff and Class Members under the FTC Act HIPAA, the CMIA, among other laws, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA software in order to safeguard Plaintiff's and Class Members' PII/PHI.

111. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

112. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

113. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII/PHI.

114. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

115. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy

116. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

117. Plaintiff and Class Members had a reasonable and legitimate expectation of privacy in the PII/PHI that Defendants disclosed without authorization.

118. Defendants owed a duty to Plaintiff and Class Members to keep their PII/PHI confidential.

119. Defendants failed to protect and release to unknown and unauthorized third parties the PII/PHI of Plaintiff and Class Members.

120. By failing to keep Plaintiff's and Class Members' PII/PHI safe, knowingly utilizing the unsecure FTA software, and disclosing PII/PHI to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class Member's privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) improperly using their PII/PHI properly obtained for a specific purpose for another purpose, or disclosing it to a third party; (iii) failing to adequately secure their PII/PHI from disclosure to unauthorized persons; and (iv) enabling the disclosure of Plaintiff's and Class Members' PII/PHI without consent.

121. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider their actions highly offensive.

122. Defendants knew, or acted with reckless disregard of the fact that, the FTA software was vulnerable to data breaches prior to the Data Beach.

123. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PII/PHI was unduly frustrated and thwarted, and caused damages to Plaintiff and Class Members.

124. In failing to protect Plaintiff's and Class Members' PII/PHI, and in disclosing Plaintiff's and Class Members' PII/PHI, Defendants acted with malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

125. Plaintiff seeks injunctive relief on behalf of the Classes, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to

Plaintiff and Class Members. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Classes.

COUNT IV
Breach of Confidence

126. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Classes.

127. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendants.

128. Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

129. Plaintiff and Class Members provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII/PHI to be disseminated to any unauthorized third parties.

130. Plaintiff and Class Members provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII from unauthorized disclosure.

131. Defendants voluntarily received in confidence Plaintiff's and Class Members' PII/PHI with the understanding that PII/PHI would not be disclosed or disseminated to unauthorized third parties or to the public.

132. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII/PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

133. As a proximate result of such unauthorized disclosures, Plaintiff and Class Members suffered damages.

134. But for Defendants' disclosure of Plaintiff's and Class Members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been compromised, stolen, viewed, access, and used by unauthorized third parties.

135. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' PII/PHI. Defendants knew or should have known that their methods of accepting, storing, transmitting and using Plaintiff's and Class Members' PII/PHI was inadequate.

136. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

137. As a direct proximate result of such unauthorized disclosures, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Breach of Contract

138. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

139. Plaintiff and Class Members provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII/PHI from unauthorized disclosure.

140. Plaintiff and the Class Members are parties to contracts with Health Net and/or intended third party beneficiaries of sub-contracts between Health Net and Accellion. Under the circumstances, recognition of a right to performance by Plaintiff and the Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiff and the Class Members the benefit of the performance promised in the contracts.

141. Defendants breached these agreements, which directly and/or proximately caused Plaintiff and the Class Members to suffer substantial damages.

142. Accordingly, Plaintiffs and Class Members are entitled to damages, restitution, disgorgement of profits and other relief in an amount to be proven at trial.

COUNT VI

Violation of the California Consumer Privacy Act, Cal. Civil Code §§ 1798.100, *et seq.*

143. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Classes.

144. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII/PHI that Plaintiff and Class Members provided to Defendants.

145. Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

146. Plaintiff and Class Members provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII/PHI from unauthorized disclosure.

147. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII/PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

148. Through the above-detailed conduct, Defendants violated California Civil Code section 1798.150 by failing to prevent Plaintiff's and Class Members' nonencrypted PII/PHI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

149. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' PII/PHI, including, among others, names, dates of birth, Social Security numbers, and medical and insurance information, was subjected to unauthorized access and exfiltration, theft, and disclosure.

150. Plaintiff seeks injunctive relief on behalf of the Classes as well as other equitable relief. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Classes.

151. In accordance with Civil Code section 1798.150(b), Plaintiff will serve Defendants with notice of violation of Civil Code section 1798.150(a) and a demand for relief. If Defendants fail to properly respond to Plaintiff's notice letter or agree to timely and adequately rectify the violations detailed above, Plaintiff will also seek actual, punitive, and statutory damages, as well as restitution, attorneys' fees and costs, and any other relief the Court deems proper.

COUNT VII
Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*

152. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Classes.

153. Defendants have engaged in unfair competition within the meaning of California Business & Professions Code section 17200, *et seq.*, because Defendants' conduct, as described herein, violated the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*, California Confidentiality in Medical Information Act ("CMIA"), Cal. Civ. Code. §§ 56, *et seq.*, and California's HIV Disclosure Laws, Cal. Health & Safety Code § 120980. Further, Defendants breached their duties pursuant to the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1302d, *et seq.*, to implement reasonable safeguards to protect Plaintiff's and Class Member's PII/PHI.

154. Plaintiff has standing to pursue this claim because they have been injured by virtue of the wrongful conduct alleged herein.

155. The Unfair Competition Law is, by its express terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes and/or common law remedies, such as those alleged in the other Counts of this Complaint. *See* Cal. Bus. & Prof. Code § 17205.

156. As a direct and proximate cause of Defendants' conduct, which constitutes unlawful business practices as alleged herein, Plaintiff and Class Members have been damaged and suffered ascertainable losses due to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

157. Plaintiff and Class Members are thereby entitled to recover restitution and equitable relief, including disgorgement or ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, filing fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

COUNT VIII

Violation of the California Confidentiality in Medical Information Act, Cal. Civ. Code §§ 56, *et seq.*

158. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

159. This cause of action is brought pursuant to the California Confidentiality in Medical Information Act ("CMIA"), Cal. Civ. Code. §§ 56, *et seq.* At all times material herein Health Net has been subject to the requirements of the CMIA. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05.

160. The CMIA requires that, except in limited circumstances expressed in the statute, prior to disclosing a patient's confidential medical information Health Net must obtain each patient's written authorization. Cal. Civ. Code § 56.11. Health Net did not obtain Plaintiff's or Class Members' express written consent in the statutorily mandated form before disclosing their medical information. Health Net's disclosure also was not permitted under any of the permissive or mandatory exceptions set forth in the CMIA. Cal. Civ. Code § 56.10. Health Net is also liable for any further disclosures of Plaintiff's and Class Members' medical information. Cal. Civ. Code §§ 56.13-14.

161. The CMIA also prohibits the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential medical information. Cal. Civ. Code § 56.101. Health Net has violated the CMIA by negligently creating, maintaining, preserving, storing, abandoning, destroying, or disposing of Plaintiff's and Class Members' medical information. Health Net's negligent acts and omissions caused Plaintiff's and Class Members' confidential medical information to be released.

162. As a direct and proximate result of Health Net's conduct, Plaintiff and Class Members are entitled to compensatory damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Health Net's violations of the CMIA, as well as attorneys' fees and costs

of suit. Cal. Civ. Code. § 56.35-36. Plaintiff and Class Members are also entitled to all necessary injunctive and declaratory relief necessary to bring Health Net's medical privacy practices into compliance with the CMIA to prevent further unauthorized uses and disclosures of their confidential medical information.

COUNT IX
Violation of the California HIV Disclosure Laws, Cal. Health & Safety Code § 120980

163. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

164. Among other things, California's Health & Safety Code prohibits the disclosure of HIV related information, including a patient's HIV status and test results. Cal. Health & Safety Code § 120980. Prior to disclosing Plaintiff's and Class Members' HIV-related health information, Defendants did not obtain any express written consent required by the statute. Defendants' disclosure of its patients' HIV status, test results, and treatment along with their personal identifying characteristics, is a negligent, willful, and malicious violation of the Health & Safety Code section 120980.

165. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have had their HIV related medical information, HIV status, and test results disclosed to third-parties without their express written authorization and have suffered damages as described in this Complaint. Accordingly, Health Net is liable for "all actual damages, including damages for economic, bodily, or psychological harm." Cal. Health & Safety Code § 120980(d). Additionally, Defendants are liable for civil penalties, fines, costs and attorneys' fees as permitted under the statute.

COUNT X
Violation of the Constitutional Right to Privacy
California Constitution, Art. 1, § 12

166. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

167. Plaintiff and Class Members have a constitutionally protected privacy interest in their confidential medical information.

168. Plaintiff and Class Members have a reasonable expectation of privacy in their confidential medical information.

169. Defendants violated that constitutionally protected right to privacy by disclosing Plaintiff's and Class Members' confidential medical information to third-parties. As a result of Defendants' unlawful conduct alleged herein, the privacy rights of Plaintiff and Class Members have been violated, and Plaintiff and Class Members have been harmed as a result thereof. Accordingly, Plaintiff and Class Members are entitled to compensatory and punitive damages, attorneys' fees.

COUNT XI
Declaratory Relief
28 U.S.C. § 2201

170. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

171. An actual controversy has arisen and now exists between Plaintiff and the putative Classes on the one hand, and Defendants on the other, concerning Defendants' failure to protect Plaintiff's and Class Members' PII/PHI in accordance with applicable state and federal regulations and the agreements between the parties. Plaintiff and the Class Members contend that Defendants failed to maintain adequate and reasonable privacy practices to protect their PII/PHI while on the other hand, Defendants contend they have complied with applicable state and federal regulations and its agreements with Plaintiff and Class Members to protect their PII/PHI.

172. Accordingly, Plaintiff and Class Members entitled to and seek a judicial determination of whether Defendants have performed, and are performing, their statutory and contractual privacy practices and obligations necessary to protect and safeguard Plaintiff's and Class Members' PII/PHI from further unauthorized, access, use, and disclosure, or insecure disposal.

173. A judicial determination of the rights and responsibilities of the parties over Defendants' privacy practices is necessary and appropriate at this time so that: (1) that the rights of the Plaintiff and the Classes may be determined with certainty for purposes of resolving this action; and (2) so that the Parties will have an understanding of Defendants' obligations in the future given its continuing legal obligations and ongoing relationships with Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of theirself and on behalf of the Classes, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23 against Defendants, appointing Plaintiff as Class Representative of the Classes, and Kaplan Fox & Kilsheimer LLP as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Classes have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATED: April 23, 2021

KAPLAN FOX & KILSHEIMER LLP

By: /s/ Matthew B. George
Matthew B. George

Laurence D. King
Matthew B. George
Mario M. Choi
1999 Harrison Street, Suite 1560
Oakland, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com
mchoi@kaplanfox.com

KAPLAN FOX & KILSHEIMER LLP
Joel B. Strauss (*pro hac vice* to be filed)
850 Third Avenue, 14th Floor
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
jstrauss@kaplanfox.com

Attorneys for Plaintiffs